Remarks

This responds to the final Office action mailed October 11, 2006 ["the Action"]. Reconsideration of the application is respectfully requested in view of the following remarks. Claims 1-20 are pending in the application. No claims have been allowed. No claims are amended. Claims 1, 2, and 13 are independent.

Cited Art

U.S. Patent No. 6,263,435 to Dondeti et al. ("Dondeti") is entitled "Dual Encyrption Protocol for Scalable Secure Group Communication."

U.S. Patent No. 6,772,331 to Hind ("Hind") is entitled "Method and Apparatus for Exclusively Pairing Wireless Devices."

Claims 1-20 Should be Allowable

The Action rejects claims 1-20 under 35 U.S.C. § 103(a) as being unpatentable over Hind in view of Dondeti. Applicants respectfully submit the claims in their present form are allowable over the cited art. To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. (MPEP § 2142.)

The Action fails to make a establish a *prima facie* case of obviousness. Accordingly, applicants request that all rejections be withdrawn.

Claim 2

Claim 2 recites, in part:

> [A] trust group, *the trust group comprising a group of devices*, . . .
> . . .
> transmitting a trust group membership certificate signed by the branding device to the security-uninitialized device via the secured network medium, *the trust group membership certificate containing a signed group name as well as a signed key identifying the security-uninitialized device such that, when the*

> *security-uninitialized device sends the trust group certificate to a branded device* which is a member of the trust group, the trust group certificate is validated by the branded device, and *the branded device verifies that the security-uninitialized device identified in the trust group membership certificate is a member of the trust group* of devices referred to by the group name; and

[Emphasis added.] For example, the Application, at page 35, line 25 to page 36, line 35, describes one example of information contained in a trust group certificate. In the example, the certificate contains information identifying a public key for the group [Application, at page 36, line 22] and the a public key for the device [Application, at page 36, line 15], which in the example is a CD Player. Additionally, at page 36, line 35, the Application notes that the public key can be used as the trust group name.

The application goes on to describe the use of the trust group membership certificate in this example:

> When the time comes for the CD to talk directly to the speaker a key exchange happens. The CD sends over its public key and the group membership certificate. The speaker does the same. Both devices are thus able to see that they are members of the same group as certified by the branding device that they have both been instructed to trust. As such the two devices will be willing to communicate with each other.

[Application, at page 36, line 38 to page 37, line 2.] *However, neither Hind nor Dondeti either teaches or suggests a "trust group membership certificate" for a "trust group comprising a group of devices" such that "when the security-uninitialized device sends the trust group certificate to a branded device . . . the branded device verifies that the security-uninitialized device identified in the trust group membership certificate is a member of the trust group* of devices."

Hind cannot teach or suggest the above-quoted language of claim 2 because Hind does not, by the Office's own admission, teach a "trust group certificate." In its rejection of claim 2, the Action cites to column 10, lines 18-29 of Hind for the proposition that Hind teaches the above-quoted "trust group membership certificate." However, this allegation contradicts the statements of previous Actions received in this application, which state, for example, "Hind does not specifically disclose that the certificate is a trust group membership certificate." [Action of May 16, 2006, at page 3; Action of October 20, 2005, at page 3.] Indeed, it is for this proposition that the previous Action utilized language of Butt. For at least this reason,

Applicants disagree with the allegation that Hind either teaches or suggests the language of claim 2 quoted above.

Additionally, Dondeti does not teach or suggest the above-quoted language of claim 2, because Dondeti discloses hosts receiving authorization certificates only for the purpose of receiving multicast messages. While Applicants note that the Action cites to Hind for the above-quoted language in the rejection of claim 2, Applicants also note that the language of claim 19, which is similar to the language quoted above, is rejected over column 4, line 57 to column 5, line 21 of Dondeti. It is for this reason that Applicants address the relation to Dondeti to this language of claim 2.

Like Hind, Dondeti does not teach or suggest the above-quoted language of claim 2, however. Dondeti is directed toward a system for multicasting. [*See*, Dondeti, at column 1, line 8.] In particular, Dondeti's system uses a "hierarchical subgrouping of multicast members" in order to provide for scalable, secure multicasting. [*See*, Dondeti, at column 2, lines 43-46.] Donedti does this by using two types of keys in a scenario where a user sends an encrypted message to one or more members of groups. [*See* Dondeti, at column 4, lines 28-39.]

In particular, the cited section of Dondeti is describes the process for joining a new "host" to a secure multicast group. [Dondeti, at colum n 4, lines 58-60.] As Donedti describes, "after the new host's membership is validated, [a] sender generates message 104, containing a number of items including an authorization certificate 56." [Dondeti, at column 5, lines 19-21.] This authorization certificate contains various data, including "the new host's identity . . ., the corresponding [subgroup manager]'s identity and the keygroup identity." [Dondeti, at column 5, lines 24-25.] In addition, "[the] Sender . . . also sends the top level KEK encryption key 60 to the joining host. This KEK corresponds to the keygroup identity that [the host] is now a part of." [Dondeti, column 5, lines 30-32.]

However, while Dondeti describes sending this information to a host during the joining process, Dondeti's description of the use of such information is limited to receiving messages from a sender during multicast. This is described in the passage of Dondeti entitled "Secure Communication":

> The sender generates a data encryption key (DEK) to be used in a conventional encryption algorithm. . . . The sender sends the multicast data encrypted with the DEK to the group. Next, the sender computes a one-way hash function of the data and sends the hash value (HV) along with the DEK to

> multicast members securely. The members also compute the hash value of multicast data and compare it to the HV received, to verify the integrity of the data.
>
> While the encrypted multicast data is sent through traditional multicast channels, the DEKs are distributed via the key distribution tree. . . . All the members of the multicast group with a local subgroup key and the corresponding KEK acquire the DEK and HV. The DEK is used by the members to decrypt the multicast data and HV is used to verify the integrity of multicast data.

[Dondeti, at column 6, line 56 to column 7, line 17.]

In contrast to the language of claim 2, Dondeti does not describe a host using either information from the received authorization certificate or the received KEK key in order to *send* any information, nor to authenticate that it (the host) is a member of any group. Indeed, the structure of Dondeti *teaches away* from such a use, as it is directed toward sending hosts information (during the joining process) to allow the host to receive *multicasted* messages. If such a host were to desire to *send* information, it would not undergo the join process described in the cited passage, if it could send information at all.

Thus, Dondeti cannot teach or suggest a "trust group membership certificate" such that "when the security-uninitialized device *sends* the trust group certificate to a branded device . . . the branded device verifies that the security-uninitialized device identified in the trust group membership certificate is a member of the trust group of devices." For at least this reason, Applicants disagree with the allegation that Hind either teaches or suggests the quoted language of claim 2.

There is no motivation to combine Hind and Dondeti in order to arrive at the above-quoted language, as Dondeti's focus on a hierarchical multicast system would change the principle of operation of Hind. As stated above, Hind has been repeatedly found to lack such a "trust group membership certificate." The present Action admits, in fact that Hind, "does not specifically disclose a method of utilizing the group membership information with toher branded devices in an open multi-access network" but instead finds this in Dondeti.

However, as discussed above, Dondeti is directed to a multicasting system. In fact, Dondeti is directed to the use of key and identifying information which can be used when *receiving* multicast messages from a sender. This is in contrast with Hind which teaches, at column 11, lines 13-48, that devices utilize a two-way communication in order to properly authenticate to each other using their certificates:

> When a first device, say a notebook computer 2003 desires to communicate with a second device 2001, the first device 2003 sends a connection request 2005 to the second device 2001. A non-secure connection 2010 is then established between the first and second devices. . . . A negotiation takes place that agrees on the need for and type of authentication, the need for encryption, the details of the cryptographic algorithms, and the details of compression if any 2020. For this use authentication is two way (both first speaker and second speaker will know each other's identity), ... As authentication proceeds, the special memory (protected storage) is asked to sign with the local device's private key (protected value) to prove said device's identity to the second device, and the special memory is asked to verify the CA's signature to validate the second device's certificate, so that the public key contained in said certificate can be trusted to verify the second device's signature. If at any point the authentication of the partner fails, the session is terminated. . . .
>
> The above-described authentication flow resulted in the exchange and validation of both devices' certificates.

As the quoted passage illustrates, Hind utilizes certificates in order to perform a two-way authentication. Indeed, if authentication of either partner fails, the session is terminated.

"If the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims *prima facie* obvious." [MPEP, § 2143.01.VI.] If Hind were to be modified to incorporate the authorization certificate and key information of Dondeti, Hind would necessarily be modified to a one-way multicasting system. As such, Hind would fail to perform two-way authentication, and would no longer perform the negotiation which underlies its pairing techniques. This means that the modification required by the action, namely using the authorization certificate and multicast key information, would change the principle of operation of Hind.

Thus, even in combination, Hind and Dondeti fail to render the claims *prima facie* obvious. As such, the combination of Hind and Dondeti fails to demonstrate a *prima facie* case for the obviousness of claim 2. Thus, claim 2, and its dependent claims 3-12, are allowable. Applicants request that the rejection of claims 2-12 be withdrawn and that claims 2-12 be allowed.

Claim 1

Claim 1 recites, in part:

> electronically imprinting the security-uninitialized device with *group membership and cryptographic key data* by the branding device via the secured network medium, *the cryptographic key data for verifying group membership information provided by other devices on the open multi-access network to the security-uninitialized device are authenticated by the branding device*; and
>
> *initializing the security-uninitialized device to use the cryptographic key data to authenticate group membership of other devices …, and to provide the security-uninitialized device's group membership to such other devices as authentication that the security-uninitialized device is a member of the trust web,*

[emphasis added]. In its rejection of claim 1, the Action cites to similar sections of Hind and Dondeti as it cited to in its rejection of claim 2. For at least this reason, as well as the reasons cited above with respect to claim 2, Hind and Dondeti, taken alone or in combination, fail to state a *prima facie* case of obviousness. Applicants also note that claim 19, which depends from claim 1, contains additional language similar to that discussed above with respect to claim 2. Thus, Claim 1, and its dependent claim 19, are allowable. Applicants request that the rejection of claims 1 and 19 be withdrawn and that the claims be allowed.

Claim 13

Claim 13 recites, in part:

> a security resolver operational when initialized with a branding public key to *authenticate trust group membership certificates* provided to the networked computing device from other devices via the network interface using the branding public key, *and further operational to inhibit interaction via the network interface with other devices not authenticated as in the trust group,…*

[emphasis added]. In its rejection of claim 13, the Action cites only to the sections cited to in its rejection of claim 2. Furthermore, the Action does not address specific language of claim 13, including the above-quoted language which is not found in claim 2. For at least this reason, as well as the reasons cited above with respect to claim 2, the Action does not demonstrate a *prima facie* case of obviousness over the combination of Hind and Dondeti for claim 13. Claim 13, as well as its dependent claims 14-18 and 20, are allowable. Applicants request that the rejection of claims 13-18 and 20 be withdrawn and that claims 13-18 and 20 be allowed.

Request for Interview

In view of the preceding amendments and remarks, Applicants believe the application to be allowable. If any issues remain, however, the Examiner is formally requested to contact the undersigned attorney at (503) 226-7391 prior to issuance of the next communication in order to arrange a telephonic interview. This request is being submitted under MPEP § 713.01, which indicates that an interview may be arranged in advance by a written request.

Conclusion

Claims 1-20 should be allowable. Such action is respectfully requested.

Respectfully submitted,

KLARQUIST SPARKMAN, LLP

One World Trade Center, Suite 1600
121 S.W. Salmon Street
Portland, Oregon 97204
Telephone: (503) 595-5300
Facsimile: (503) 595-5301

By _____
Stephen A. Wight
Registration No. 37,759